IN THE CLAIMS:
This listing replaces all prior claim listings:

1. (Currently amended) A ~~security~~ system ~~for use in a distributed network~~, comprising:

a service provider selectively accessible via a network by a plurality of end users each having an access device for accessing the network, wherein the service provider maintains a level of integrity to allow it to provide network access to an access device; and

a control mechanism disposed at a location of the service provider which accesses each of the access devices to modify stored network connection information on a corresponding access device of a corresponding end user and thereby remotely designate portions of the information as service provider-accessible only to prevent compromise of the service provider's integrity ~~access of the designated information~~ by the corresponding end user.

2. (Previously presented) The system as recited in claim 1, wherein the control mechanism can determine if an end user has accessed the service provider only accessible portions of the information.

3. (Original) The system as recited in claim 1, wherein the stored information includes a configuration file for the access device.

4. (Original) The system as recited in claim 1, wherein service provider includes a security code for the designated portions to prevent access thereof by the end users.

5. (Previously presented) The system as recited in claim 4, wherein the security code is associated with the designated portions at or before initializing the access devices.

6. (Previously presented) The system as recited in claim 4, wherein the security code is associated with the designated portions after initializing the access devices.

7. (Original) The system as recited in claim 1, wherein service provider includes security levels for the information to prevent access thereof by the end users.

8. (Previously presented) The system as recited in claim 7, wherein the security levels are associated with the designated portions at or before initializing the access devices.

9. (Previously presented) The system as recited in claim 7, wherein the security levels are associated with the designated portions after initializing the access devices.

10. (Original) The system as recited in claim 1, wherein the control mechanism includes a software program for accessing and modifying the information of the access devices and designating portions thereof to prevent access by the end users.

11. (Currently amended) A method ~~for maintaining system security for a network service provider~~, comprising the steps of:

providing a control mechanism at a network service provider for remotely accessing and modifying end user network access devices, wherein the network service provider maintains a level of integrity to allow it to provide network access to an access device;

remotely accessing the end user network access devices to modify network connection information stored on a corresponding access device and thereby remotely designate portions of the information as service provider-accessible only; and

preventing an end user of the corresponding access device from ~~accessing~~ compromising the service provider's integrity by denying end user access to the designated information on the corresponding access device.

12. (Previously presented) The method as recited in claim 11, further comprising the step of:

employing the control mechanism to determine if an end user has accessed the service provider only accessible portions of the information.

13. (Previously presented) The method as recited in claim 11, wherein the step of providing the control mechanism includes providing a software program for accessing and modifying the information of the access devices and designating portions thereof to prevent access by the end users.

14. (Previously presented) The method as recited in claim 11, wherein the step of remotely accessing and modifying the end user network devices includes remotely accessing the end user devices from a service provider's location.

15. (Previously presented) The method as recited in claim 11, wherein the information stored on the network access devices includes a configuration file for the access device.

16. (Previously presented) The method as recited in claim 11, wherein the step of preventing the end user from accessing the designated information includes employing a security code for the designated portions to prevent access thereof by the end users.

17. (Previously presented) The method as recited in claim 15, wherein the security code is associated with the designated portions at or before initializing the access devices.

18. (Previously presented) The method as recited in claim 15, wherein the security code is associated with the designated portions after initializing the access devices.

19. (Previously presented) The method as recited in claim 11, further comprising the step of assigning security for the stored information to prevent access thereof by the end users.

20. (Previously presented) The method as recited in claim 18, wherein the security levels are associated with the designated portions at or before initializing the access devices.

21. (Previously presented) The method as recited in claim 18, wherein the security levels are associated with the designated portions after initializing the access devices.